Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR05/000615

International filing date: 04 March 2005 (04.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2004-0046756
Filing date: 22 June 2004 (22.06.2004)

Date of receipt at the International Bureau: 17 May 2005 (17.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office

출 원 번 호 : 특허출원 2004년 제 0046756 호
Application Number 10-2004-0046756

출 원 일 자 : 2004년 06월 22일
Date of Application JUN 22, 2004

출 원 인 : 한국전자통신연구원 외 5 명
Applicant(s) Electronics and Telecommunications Research Institute, et al

2005 년 04 월 07 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2004.06.22

【발명의 국문명칭】 ＩＥＥＥ 802.16 ＷｉｒｅｌｅｓｓＭＡＮ기반의 휴대 인터넷 시스템에서 Ｍｕｌｔｉｃａｓｔ 서비스와 Ｂｒｏａｄｃａｓｔ 서비스에 대한 트래픽 암호화 키 관리 방법

【발명의 영문명칭】 The method to manage traffic encryption key for the multicast and broadcast services in the IEEE 802.16 WirelessMAN System

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【출원인】

【명칭】 삼성전자 주식회사

【출원인코드】 1-1998-104271-3

【출원인】

【명칭】 주식회사 케이티

【출원인코드】 2-1998-005456-3

【출원인】

【명칭】 주식회사 케이티프리텔

【출원인코드】 1-1998-098986-8

【출원인】

【명칭】 에스케이텔레콤 주식회사

【출원인코드】 1-1998-004296-6

【출원인】

【명칭】 하나로통신 주식회사

【출원인코드】 1-1998-112749-2

【대리인】

【명칭】 유미특허법인

【대리인코드】 9-2001-100003-6

【지정된변리사】 이원일

【포괄위임등록번호】 2001-038431-4

【포괄위임등록번호】 2002-036528-9

【포괄위임등록번호】 2003-082444-7

【포괄위임등록번호】 2002-031524-6

【포괄위임등록번호】 2002-062290-2

【포괄위임등록번호】 2004-014783-3

【발명자】

【성명의 국문표기】 조석헌

【성명의 영문표기】 CHO,SEOK HEON

【주민등록번호】 770127-1543416

【우편번호】 570-976

【주소】 전라북도 익산시 신동 775-21번지

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 유미특허법인 (인)

【수수료】

【기본출원료】 0 면 38,000 원

【가산출원료】 44 면 0 원

【우선권주장료】 0 건 0 원

【심사청구료】 0 항 0 원

【합계】	38,000 원

【요약서】

【요약】

IEEE 802.16 WirelessMAN기반의 무선 인터넷 시스템에서는 서비스를 안전하게 제공하기 위하여 트래픽 데이터에 대한 암호화 기능을 정의하고 있다. 트래픽 데이터에 대한 암호화 기능은 서비스의 안정성 및 망의 안정성을 위하여 필요한 기본적인 요구사항으로 대두되고 있다. IEEE 802.16 WirelessMAN 시스템에서는 이와 같은 트래픽 데이터의 암호화 및 복호화를 위하여 단말 (SS)과 기지국 (BS) 사이에 보안 키 관리 프로토콜 (PKM: Privacy Key Management) MAC 메시지들을 정의하고 있다.

본 발명은 IEEE 802.16 WirelessMAN 시스템에서 정의하고 있는 트래픽 데이터에 대한 암호화 키를 관리하는 방법에 있어서, 암호화 키들에 대한 생성, 분배 및 갱신하는 방법을 정의하기 위한 것이다. 특히, IEEE 802.16 WirelessMAN 시스템에서는 Multicast 서비스와 Broadcast 서비스용 암호화 키 갱신 및 분배 방법에 대하여 Unicast 서비스용 암호화 키 갱신 및 분배하는 방법과 동일하게 고려하고 있다. 이에 본 발명은 Multicast 서비스와 Broadcast 서비스용 암호화 키들을 보다 효율적으로 관리하기 위해서 Unicast 서비스용 암호화 키를 관리하는 방법과는 다른 방법을 제시한다. 본 발명의 결과로써 IEEE 802.16 WirelessMAN 시스템은 트래픽 데이터에 대한 암호화 키를 보다 효과적이고 유연하게 관리할 수 있게 된다.

【대표도】

도 2

【색인어】

IEEE 802.16 WirelessMAN, 트래픽 암호화 키 (TEK), 갱신

【명세서】

【발명의 명칭】

ＩＥＥＥ 802.16 ＷｉｒｅｌｅｓｓＭＡＮ기반의 휴대 인터넷 시스템에서 Ｍｕｌｔｉｃａｓｔ 서비스와 Ｂｒｏａｄｃａｓｔ 서비스에 대한 트래픽 암호화 키 관리 방법{The method to manage traffic encryption key for the multicast and broadcast services in the IEEE 802.16 WirelessMAN System}

【도면의 간단한 설명】

<1> 도 1은 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 생성, 분배 및 갱신하는 절차도,

<2> 도 2는 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 갱신하는 방법도,

<3> 도 3은 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신하기 위한 추가 PKM 파라미터 테이블,

<4> 도 4는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 갱신 절차도,

<5> 도 5는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 갱신 방법도,

<6> 도 6은 본 발명에서 적용되는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 응답 (Key Reply) 메시지 테이블,

<7> 도 7은 본 발명에서 제안하는 트래픽 암호화 키 관련 파라미터 (TEK-parameters)들의 테이블,

<8> 도 8은 본 발명에서 제안하는 Key Update Command 메시지의 테이블,

<9> 도 9는 본 발명에서 제안하는 Key push modes 테이블,

<10> 도 10은 본 발명에서 제안하는 Key Update Command 메시지의 HMAC-Digest 생성 시 사용되는 입력키 테이블,

<11> 도 11는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신하는데 있어서 비정상적인 경우의 절차도,

<12> 도 12는 본 발명에서 제안하는 단말의 트래픽 암호화 키 요청 상황에 따른 Key Reply 메시지에 포함되어 전송되는 TEK-Parameters 정보 테이블,

<13> 도 13은 본 발명에서 제안하는 기지국이 트래픽 암호화 키 갱신을 시작하고 분배하는 방식에서의 트래픽 암호화 키 상태 머신 흐름도,

<14> 도 14는 본 발명에서 제안하는 기지국이 트래픽 암호하 키 갱신을 시작하고 분배하는 방식에서의 트래픽 암호화 키 상태 천이 테이블이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<15> 본 발명의 목적은 IEEE 802.16 WirelessMAN 시스템 기반의 무선 인터넷 시스템에서 Multicast 서비스용 또는 Broadcast 서비스용 트래픽에 대한 암호화 키를

관리하는 방법을 제안한다.

<16> 본 발명의 결과로써, 해당 시스템에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 (TEK : Traffic Encryption Key)를 갱신 및 분배하는데 있어서 무선 구간 신호 채널의 사용 부하를 감소시킬 수 있다. 즉, Multicast 서비스나 Broadcast 서비스를 제공받고 있는 모든 가입자들이 트래픽 암호화 키 갱신 요청을 하고 이에 대하여 기지국이 동일한 트래픽 암호화 키를 모든 가입자들에게 개별적으로 응답을 하는 방법 대신에 기지국이 내부 이벤트로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하고 이를 방송 채널을 통하여 모든 가입자들에게 동시에 분배하는 방법을 채택함으로써, 위 두 서비스용 트래픽 암호화 키를 갱신하는데 있어서 무선 구간 신호 채널의 사용 부하를 현저하게 감소시킬 수 있다. 이에 IEEE 802.16 WirelessMAN 시스템 기반의 무선 인터넷 시스템은 Multicast 서비스나 Broadcast 서비스를 안전하게 끊임없이 제공할 수 있을 뿐만 아니라 신호 채널과 관련된 무선 자원을 보다 효율적으로 사용 가능할 수 있게 되어 전체 시스템하의 성능을 높일 수 있다.

<17> 본 발명이 속하는 기술 분야는 데이터 트래픽의 보안 분야로, 적용 대상이 되는 시스템은 IEEE 802.16 WirelessMAN 시스템이다. IEEE 802.16 WirelessMAN 시스템에서 제공하는 Mulitcast 서비스 또는 Broadcast 서비스용 트래픽 암호화 키를 효율적으로 관리하기 위한 방법에 관한 것이다.

<18> 기존 IEEE 802.16 WirelessMAN 시스템에서는 트래픽 데이터를 암호화하기 위해서 모든 트래픽 암호화 키를 생성하고 분배하는 방식을 정의하였다. 또한, 이 트

래픽 암호화 키 또한 보안을 유지하기 위해서 일정 시간이 지나면 갱신하여 새로운 트래픽 암호화 키를 생성 및 분배한다. 이를 통해, 단말과 기지국은 동일한 트래픽 암호화 키를 공유한다. 이와 같이 인증 및 보안 관련 기능을 수행하기 위해서, 단말과 기지국은 PKM-REQ (Privacy Key Management Request) 메시지와 PKM-RSP (Privacy Key Management Response) 메시지를 사용한다. 단말은 PKM-REQ 메시지 중 한 메시지인 Key Request 메시지를 기지국으로 전송함으로써 새로운 트래픽 암호화 키에 대한 할당을 요구하거나 트래픽 암호화 키 갱신을 요구한다. 이 메시지를 수신한 기지국은 응답으로서 트래픽 암호화 키 할당이나 갱신이 성공하였을 경우에는 PKM-RSP 메시지 중 한 메시지인 Key Reply 메시지를, 실패하였을 경우에는 Key Reject 메시지를 해당 단말로 전송한다. 이와 같은 일련의 트래픽 암호화 키 할당 및 갱신 절차를 통해 단말과 기지국 사이에서 공유하게 된 트래픽 암호화 키를 이용하여 무선 구간의 트래픽 데이터를 암호화 및 복호화하여 송, 수신하게 된다.

<19> IEEE 802.16 WirelessMAN 시스템에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신 방법은 Unicast 서비스용 트래픽 암호화 키 갱신 방법과 동일하다. 하지만, Unicast 서비스용 트래픽 암호화 키 갱신 방법과 동일한 절차로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하는 것은 무선 채널 자원을 불필요하게 사용하는 제한점이 있다. 이에 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신에 따른 무선 채널 자원을 효과적으로 감소하는 절차가 필요하다.

【발명이 이루고자 하는 기술적 과제】

<20> 본 발명은 상기에 기술한 바와 같이, IEEE 802.16 WirelessMAN 시스템에서 기존에 정의하였던 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신하기 위해 사용되는 신호 메시지의 무선 채널 구간에서 불필요한 사용을 줄이기 위해서 새로운 갱신 방법을 제안하고자 한다. 즉, 이 발명의 궁극적인 목적은 Multicast 서비스나 Broadcast 서비스용 트래픽 데이터를 끊임없이 안전하게 전달하기 위해 이런 서비스들의 트래픽 암호화 키를 주기적으로 갱신하는데, 이와 같이 트래픽 암호화 키를 갱신할 때 사용되는 메시지를 방송 신호 채널을 사용하여 전달함으로써 기존 방식보다 훨씬 적은 양의 신호 무선 자원으로도 효과적으로 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 분배하기 위함이다.

【발명의 구성】

<21> 제 1도는 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 생성, 분배 및 갱신하는 절차도이다.

<22> IEEE 802.16 WirelessMAN 시스템에서 단말 (SS, 101)은 임의의 Multicast 서비스나 Braodcast 서비스를 받기 전에 우선 해당 트래픽 데이터를 암호화는데 필요한 트래픽 암호화 키를 분배받아야 한다. 여기에서 모든 Multicast 서비스나 Broadcast 서비스에는 각각의 서비스 트래픽 데이터를 암호화하기 위해 개별적인 트래픽 암호화 키가 존재한다. 다시 말해서, 모든 Multicast 서비스용 트래픽 암호화 키가 서로 다르고 Broadcast 서비스용 트래픽 암호화 키와도 다르기 때문에, 하

나의 트래픽 암호화 키를 단말이 안다고 할지라고 다른 Multicast 서비스를 제공받을 수 없는 것이다.

<23> 트래픽 암호화 키, 트래픽 암호화 키 일련번호, 트래픽 암호화 키 유효시간, 암호화 알고리즘 등을 포함하는 집합을 하나의 SA (Security Association)으로 표현한다. 이 SA에는 식별자 기능을 하는 SA-ID도 포함하고 있다. Multicast 서비스나 Broadcast 서비스는 서로 다른 하나의 SA와 관련되어 있다. 다시 말해서, 임의의 동일한 Multicast 서비스를 제공받는 단말들은 동일한 하나의 SA 정보를 가지고 있고 Broadcast 서비스를 제공받는 단말들도 동일한 하나의 SA 정보를 가지고 있지만, 이 들 Multicast 서비스나 Broadcast 서비스와 관련된 SA가 서로 독립적이기 때문에 이들 개별 서비스 하나당 하나의 SA와 관련있다고 간주할 수 있다.

<24> 단말이 전송하는 해당 서비스의 트래픽 암호화 키 분배 요청 메시지의 MAC 헤더에는 Primary Management CID가 사용된다. Primary Management CID는 기지국이 단말의 초기 접속시 단말마다 고유하게 할당해주는 CID로써 단말을 구별해줄 수 있다. 이 Key Request 메시지에는 해당 서비스와 관련된 SA의 식별자인 SA-ID가 포함되어 있어서 그림 예에서와 같이 n번째 SA 즉 트래픽 암호화 키와 그에 따른 정보들을 요청하는 것이다.

<25> 이 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 생성 및 분배 요청 메시지인 Key Request 메시지를 수신한 기지국은 해당 서비스용으로 기존에 생성하였던 트래픽 암호화 키를 요청하였던 단말로 Key Reply 메시지를 통해 전송한다 (S112). 단말이 n번째 SA를 요구하였기 때문에 기지국은 n번째 SA들을 응답

메시지인 Key Reply 메시지에 포함시켜 전송하는 것이다. 이 때의 Key Reply 메시지의 MAC 헤더에는 트래픽 암호화 키를 요청하였던 단말에게만 전송해야 하므로 Key Request 메시지의 MAC 헤더에 포함되었던 Primary Management CID를 그대로 사용한다. 이로써 단말이 임의의 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 최초로 분배받는 절차가 완료되는 것이다.

<26> Key Reply 메시지를 통해 수신한 *n*번째 SA의 기지국이 *x*번째로 생성한 트래픽 암호화 키를 가지고 단말은 해당 서비스의 트래픽 데이터를 복호화하는 것이다. 또한, *x*번째로 생성된 트래픽 암호화 키를 Key Reply 메시지로 분배 받자마자 해당 트래픽 암호화 키의 실제 유효 시간이 시작된다 (111). 이 후 단말은 끊임없이 안전하게 트래픽 서비스를 제공받기 위해서 주기적으로 트래픽 암호화 키를 갱신해야 한다. 이를 위해 단말은 내부적으로 TEK Grace Time (112)을 관리한다. 이 TEK Grace Time은 이전에 할당 받았던 트래픽 암호화 키가 만료되기 전에 단말이 트래픽 암호화 키 갱신 요청을 유발하는 시점을 의미한다. 즉, 단말은 이 TEK Grace Time이 작동하게 되면 트래픽 암호화 키 상태 머신으로 TEK Refresh Timeout (S121) 이벤트를 발생시킨다.

<27> TEK Refresh Timeout 이벤트로 인해 단말은 기지국으로 트래픽 암호화 키 갱신 및 분배 요청 메시지인 Key Request (S131) 메시지를 전송한다. Key Request 메시지의 MAC 헤더에는 최초로 트래픽 암호화 키를 요청하였던 Key Request 메시지 (S111)의 MAC 헤더에서 포함되었던 Primary Management CID를 사용한다. Key Request 메시지에는 해당 Multicast 서비스나 Broadcast 서비스에 관련된 SA

(Security Association)의 식별자 (SA-ID)가 포함되어 있다. *n*번째 SA에서 새로운 트래픽 암호화 키를 요구하기 때문에 Key Request 메시지에 포함된 SA-ID값은 *n*이다.

<28> Key Reuqest 메시지를 수신한 기지국은 응답 메시지로써 트래픽 암호화 키를 생성하고 이 트래픽 암호화 키를 Key Reply 메시지에 포함시켜 해당 단말로 전송한다 (S132). Key Reply 메시지의 MAC 헤더에도 트래픽 암호화 키를 최초로 분배하였던 Key Reply 메시지 (S112)의 MAC 헤더에서 사용하였던 Primary Management CID를 사용한다. Key Request 메시지에 SA-ID값이 *n*이기 때문에 Key Reply 메시지에는 *n*번째의 SA가 포함된다. 이 SA에는 기지국이 *x+1*번째로 생성한 트래픽 암호화 키가 존재한다. 단말이 *x+1*번째로 생성된 트래픽 암호화 키를 Key Reply 메시지로 분배받자마자 해당 *x+1*번째의 트래픽 암호화 키 실제 유효 시간이 시작된다 (113). 이후부터 제공받은 해당 서비스 데이터는 *x+1*번째의 트래픽 암호화 키를 가지고 복호화하는 것이다. 이로써, Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 분배하는 절차가 완료되는 것이다.

<29> 이와 같은 기존의 트래픽 암호화 키 분배 알고리즘에서는 해당 Multicast 서비스나 Broadcast 서비스를 제공받은 모든 단말이 동시에 트래픽 암호화 키를 요청하기 위해서 무선 대역을 요구하고 Key Request를 전송한다. 또한, 기지국은 단말들로부터 수신한 Key Request 메시지들을 처리하고 그 응답으로써 Key Reply 메시지들을 모든 단말 각각에게 한 시점에 전송하게 된다. Multicast 서비스나 Broadcast 서비스에 있어서 기존의 트래픽 암호화 키 분배 알고리즘은 기지국이 이

Key Request와 Key Reply 메시지들을 처리하기 위해서 한 동안은 트래픽 데이터 서비스를 효율적으로 제공하기가 불가능하게 되어 결국 무선 자원을 비효율적으로 사용하게 된다는 단점이 있다.

<30> IEEE 802.16 WirelessMAN 시스템에서 지원하는 트래픽 암호화 키를 갱신하기 위해서 32바이트의 Key Request 메시지와 최대 90바이트의 Key Reply 메시지가 사용되고 즉, 한 단말에게 하나의 서비스 당 트래픽 암호화 키를 갱신하기 위해서 총 122바이트의 신호 메시지가 사용된다.

<31> 제 2도는 IEEE 802.16 WirelessMAN 시스템에서 정의된 트래픽 암호화 키를 갱신 및 분배하는 방법에 관한 그림이다.

<32> 여기에 도시된 단말들은 하나의 동일한 Multicast 서비스나 Broadcast 서비스를 현재 제공받고 있는 단말들이다. 하나의 Multicast 서비스나 Broadcast 서비스가 *n*번째 SA와 관련되어 있다고 가정한다. 모든 단말들 (SS1 ~ SS*z*)은 각각 내부적으로 저장하고 있는 TEK Grace Time에 의해 TEK Refresh Timeout 이벤트가 발생하고 *n*번째 SA의 트래픽 암호화 키를 갱신받기 위해서 Key Request 메시지를 기지국으로 전송한다 (S211, S221, S231, S2*z*1). 모든 단말들의 *n*번째 SA에 해당하는 TEK Grace Time 시점이 동일하기 때문에 모든 단말로부터의 Key Request 메시지들이 거의 한 순간에 기지국으로 전송된다. 이 때 모든 단말들이 Key Request 메시지에는 값이 *n*인 SA-ID를 포함한다. 하지만, 이 Key Request 메시지의 MAC 헤더에는 단말이 초기 접속 시 기지국으로부터 단말마다 고유하게 할당받은 서로 다른 Primary Management CID가 사용된다. 이처럼 *z*개의 단말이 현재 서비스를 받고 있

는 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신 요청 메시지를 전송하기 위해서 동일한 시간에 무선 채널 구간에 하나의 서비스당 *32 z* 바이트가 사용된다.

<33> *z*개의 단말로부터 *n*번째 SA의 트래픽 암호화 키 갱신 요청 메시지를 각각 수신받은 기지국은 *n*번째 SA의 트래픽 암호화 키를 갱신하고 응답 메시지로써 *n*번째 SA가 포함된 Key Reply 메시지를 모든 단말들에게 동시에 각각 전송한다 (S212, S222, S232, S2*z*2). 이 때 전송하는 Key Reply 메시지의 MAC 헤더에는 각각의 단말에게 할당된 Primary Management CID가 사용된다. 기지국은 특정 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 분배하기 위해서는 모든 단말에게 일일이 Key Reply 메시지를 전송해야 하기 때문에 무선 채널 구간에 *90 z* 바이트가 사용된다.

<34> 다시 말해서, 특정 Multicast 서비스나 Broadcast 서비스를 제공 받는 모든 단말들은 동일한 하나의 트래픽 암호화 키를 기지국으로부터 분배받아 해당 서비스 트래픽 데이터를 복호화할 때 사용한다. 하지만, 동일한 트래픽 암호화 키를 갱신하는데 있어서 모든 단말이 갱신 요청을 하고 이에 따라 기지국이 모든 단말에게 일일이 갱신된 트래픽 암호화 키를 분배하는 방식은 비효율적이다. 예를 들면, 하나의 Multicast 서비스나 Broadcast 서비스를 제공받고 있는 단말이 *z*개라면 해당 서비스용 트래픽 암호화 키를 갱신하는데 총 *122 z* 바이트가 필요하다. 이는 무선 채널의 신호 자원의 과다한 낭비이다.

<35> 즉, 이처럼 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱

신하는데 있어서, Unicast 서비스용 트래픽 암호화 키를 갱신하는 방법처럼 모든 단말이 해당 서비스의 트래픽 암호화 키 갱신을 유발하여 요청하고, 이 요청에 대하여 기지국이 모든 단말에게 분배하는 것은 임의의 짧은 순간에 무선 채널의 신호 자원을 낭비하고 기지국의 불필요한 처리량을 야기한다.

<36> 제 3도는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신하기 위한 암호 관련 PKM 파라미터 테이블이다 (300).

<37> 여기에서 M&B (Multicast & Broadcast) TEK Grace Time은 기지국이 내부적으로 저장하고 있는 파라미터로써 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키가 만료되기 전 기지국이 해당 서비스의 트래픽 암호화 키를 갱신을 시작하는 시점을 의미한다. 이 M&B TEK Grace Time은 단말이 트래픽 암호화 키가 만료되기 전 갱신을 시작하는 시점을 의미하는 TEK Grace Time보다 큰 값을 가져야한다. 왜냐하면, Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키 갱신을 단말이 아닌 기지국이 먼저 시작해야 하기 때문이다.

<38> 제 4도는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 생성, 분배 및 갱신하는 절차도이다.

<39> 단말이 임의의 Multicast 서비스나 Broadcast 서비스를 받기 전에 우선 해당 서비스 트래픽 데이터를 복호하는데 필요한 트래픽 암호화 키를 분배받아야 한다. 이와 같은 최초로 해당 서비스의 트래픽 암호화 키를 분배받는 절차 (S411, S412)는 제 1도에서 단말의 최초 트래픽 암호화 키 분배 절차 (S111, S112)와 동일하다. 하지만, 기지국으로부터 전송되는 Key Reply 메시지에는 트래픽 암호화 키를 암호

화하기 위해서 필요한 GKEK가 포함되어 있다. GKEK는 단말과 기지국이 미리 공유한 단말의 인증키로 암호화되어 있다.

<40> *n*번째 SA의 기지국이 *x*번째로 생성한 해당 서비스의 트래픽 암호화 키가 포함된 Key Reply 메시지를 단말이 수신받음으로써, *x*번째의 트래픽 암호화 키의 실제 유효 시간이 시작되고 (411), 이 유효 시간동안 단말은 해당 서비스를 제공받을 때 *x*번째 트래픽 암호화 키를 가지고 트래픽 데이터를 복호한다.

<41> 해당 서비스의 트래픽 데이터를 끊임없이 안전하게 기지국이 단말에게 제공하기 위해서 *n*번째 SA의 트래픽 암호화 키를 주기적으로 갱신해야 한다. 하지만, 제 1도에서의 IEEE 802.16 WirelessMAN 시스템에서처럼 단말이 트래픽 암호화 키 갱신을 유발하지 않고, 본 발명에서 제안하는 바는 기지국이 해당 서비스 트래픽 암호화 키를 주기적으로 갱신하는 것이다. 이를 위해 기지국은 내부적으로 제 3도에서 언급하였던 M&B TEK Grace Time 파라미터를 관리하고 두 종류의 Key Update Command 메시지를 사용한다. 기지국은 이 M&B TEK Grace Time 시간 전에 해당 서비스를 제공받고 있는 모든 단말들에게 개별적으로 Key Update Command 메시지를 전송한다 (S421). 이 메시지를 통해서 모든 단말들은 다음 트래픽 암호화 키를 암호화하는 필요한 32 바이트의 GKEK (Group Key Encryption Key)를 분배받게 된다. 기지국이 GKEK를 모든 단말에게 분배할 때 한 시점에 집중되지 않게 하기 위해서 기지국 내부적으로 Key Update Command 메시지를 시간적으로 분산시켜 개별적으로 전송한다. 즉, 이 때 전송하는 Key Update Command 메시지의 MAC 헤더에는 Primary Management CID가 사용되고, GKEK는 해당 단말과 공유하고 있는 인증키인 AK를 사

용하여 암호화되어 전송된다. 이 후, Multicast 서비스나 Broadcast 서비스별로 이 M&B TEK Grace Time (421)시점이 되면 해당 서비스 트래픽 암호화 키 상태 머신으로 M&B TEK Refresh Timeout 이벤트를 발생시킨다 (S422). 이 M&B TEK Refresh Timeout 이벤트로 인해 트래픽 암호화 키 상태 머신에게 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 새롭게 갱신하게 된다.

<42> 기지국은 모든 단말에게 *n*번째 SA의 갱신된 *x+1*번째 트래픽 암호화 키를 포함한 Key Update Command 메시지를 한 번에 방송적으로 전송한다 (S423). 즉, 이 Key Update Command 메시지는 Broadcast Connection을 통해 전송되며, 이 메시지의 MAC 헤더에는 Broadcast CID가 사용된다. 이 때 전송되는 트래픽 암호화 키는 전에 할당받은 GKEK로 암호화되어 전송된다. 이처럼, GKEK와 트래픽 암호화 키를 포함한 두 개의 Key Update Command 메시지를 모두 수신한 단말은 내부적으로 관리하고 있는 TEK Grace Time이 동작하지 않게 된다 (422). 즉, Multicast 서비스나 Broadcast 서비스를 제공받는 단말은 Unicast 서비스와 달리 해당 서비스에 대한 특별한 트래픽 암호화 키 요청없이 트래픽 암호화 키를 분배받게 되는 것이다. 이 후, *x* 번째 트래픽 암호화 키의 유효 시간이 만료되면 해당 *x+1*번째의 트래픽 암호화 키 실제 유효 시간이 시작된다 (412). 이 후부터 제공받은 해당 서비스 데이터는 *x+1*번째의 트래픽 암호화 키를 가지고 복호화하는 것이다.

<43> 본 특허에서 제안하는 Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키를 갱신하기 위해서 Key Update Command 라는 메시지를 두 번 사용한다. 처음은 다음 유효 시간 동안 사용될 트래픽 암호화 키를 암호하는 사용될 GKEK를

분배하기 위한 것으로 이 때에는 최대 66바이트의 Key Update Command 메시지를 기지국은 M&B TEK Grace Time 시간 이전에 해당 서비스를 제공받고 있는 모든 단말 각각에게 Primary Management Connection을 통해 전송한다. 기지국이 내부적으로 관리하고 있는 타이머인 M&B TEK Grace Time 시점에 기지국은 모든 단말에게 다음 유효 시간동안 사용될 트래픽 암호화 키를 모든 사람에게 한 번의 Key Update Command 메시지를 방송적으로 분배한다, 다음 트래픽 암호화 키가 포함된 Key Update Command 메시지는 최대 70바이트 사이즈이다.

<44> 제 5도는 본 발명에 적용되는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 분배하는 방법에 관한 그림이다.

<45> 여기에 도시된 단말들은 하나의 동일한 Multicast 서비스나 Broadcast 서비스를 현재 제공받고 있는 단말들이다 (SS1 ~ SSz). 하나의 Multicast 서비스나 Broadcast 서비스가 n번째 SA와 관련되어 있다고 가정한다. 기지국은 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 자체적으로 갱신하기 위해서 내부적으로 그림 3과 그림 4에서 언급한 바와 같이 M&B TEK Grace Time을 관리하고 있는데, 이 M&B TEK Grace Time 시점 이전에 기지국은 모든 단말 각각에게 Primary Management Connection을 통해 다음 트래픽 암호화 키를 암호하는데 필요한 GKEK를 분배한다 (S511, S512, S513, S51z). 기지국은 GKEK를 분배하기 위해서 Key Update Command 메시지를 일정 시간에 걸쳐 기지국에 부하가 생기지 않도록 하나씩 전송한다. 이 때 전송하는 Key Update Command 메시지의 MAC 헤더에는 Primary Management CID가 사용된다.

<46> 이 후, M&B TEK Grace Time 시점이 되면 기지국의 트래픽 암호화 키 상태 머신에 M&B TEK Refresh Timeout 이벤트를 발생한다. M&B TEK Refresh Timeout 이벤트로 인해 기지국은 해당 서비스용 트래픽 암호화 키를 갱신하고 이를 모든 단말들에게 하나의 Key Update Command 메시지를 Broadcast Connection을 통해 전송함으로써 트래픽 암호화 키를 분배한다 (S520). 즉, 이 때 전송하는 Key Update Command 메시지의 MAC 헤더에는 모든 단말들에게 한번에 전달할 수 있는 Broadcast CID가 사용된다.

<47> 또한, 본 발명이 제안한 방식에서 기지국이 특정 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 갱신 및 z개의 단말들에게 분배하기 위해서 무선 채널 구간에서 사용되는 첫번째 Key Update Command 메시지는 총 $66 \quad z$ 바이트가 사용되고, 두번째 Key Update Command 메시지는 70바이트가 사용된다. 즉, 사용되는 신호 자원은 총 $(66 \quad z + 70)$ 바이트에 불과하다. 이에 비해, 단말이 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키 갱신을 시작하는 방식에서는 z개의 단말이 트래픽 암호화 키를 갱신하는데 총 $122 \quad z$ 바이트의 신호 자원이 필요하며 이는 비효율적이다. 또한, 기지국 입장에서 볼 때, 단말이 트래픽 암호화 키 갱신을 시작하는 방식에서는 한 순간에 MAC 메시지와 해당 SA를 생성하는데 너무나 많은 처리량이 필요하지만, 본 발명에서 제안하는 방식은 작은 처리량으로도 해당 Multicast 서비스나 Broadcast 서비스를 제공받고 있는 단말들에게 트래픽 암호화 키를 안정적으로 갱신 및 분배할 수 있다는 장점이 있다.

<48> 제 6도는 본 발명에서 적용되는 Multicast 서비스와 Broadcast 서비스용 트

래픽 암호화 키 응답 (Key Reply) 메시지의 내부 파라미터들의 테이블이다.

<49> 도 4에서와 같이 단말이 Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키 요청 시 이에 대한 응답 메시지로 기지국은 Key Reply 메시지를 전송한다 (S411, S412). 이 Key Reply 메시지에는 트래픽 암호화 키와 관련된 인증키 일련 번호를 의미하는 Key-Sequence-Number, 해당 SA의 식별자인 SA ID, 현재 트래픽 암호화 키 유효 시간과 다음 트래픽 암호화 키 유효 시간 동안 유효한 트래픽 암호화 키와 관련된 정보들인 TEK-Parameters과 이 Key Reply 메시지 인증 기능을 위한 HMAC-Digest가 포함된다.

<50> 제 7도는 본 발명에서 제안하는 트래픽 암호화 키 관련 파라미터 (TEK-Parameters)들을 표현한 테이블이다.

<51> 여기에는 GKEK가 포함된다. 이 GKEK는 Multicast 서비스나 Broadcast 서비스에서만 정의되는 파라미터로써 그룹 키 암호화 키 (Group Key Encryption Key)이다. GKEK는 트래픽 암호화 키를 암호하는 필요한 키이고, 이 GKEK도 단말에게 분배한 인증키로 암호화되어서 전송된다.

<52> 트래픽 암호화 키는 트래픽 데이터를 암호화하는데 필요한 입력 키이다. 기지국이 이 트래픽 암호화 키를 해당 서비스를 제공받고 있는 단말에게 안전하게 전송하기 위해서 트래픽 암호화 키 자체도 암호화해서 전송한다. 이를 위해서, Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키는 GKEK로 암호화하고, Unicast 서비스용 트래픽 암호화 키는 KEK로 암호화한다.

<53> 이외에 트래픽 암호화 키 유효 시간, 트래픽 암호화 키 일련 번호, 트래픽

데이터를 암호화하는데 필요한 입력 키 역할을 하는 CBC-IV가 포함된다.

<54> 특히, Multicast 서비스와 Broadcast 서비스에 있어서 Unicast 서비스와 달리 GKEK와 트래픽 암호화 키는 Multicast 서비스마다 그리고 Broadcast 서비스에서 동일하다. 즉, Multicast 서비스나 Broadcast 서비스를 제공받고 있는 모든 단말들은 동일한 GKEK와 트래픽 암호화 키를 공유하는 것이다. 이 때의 GKEK와 트래픽 암호화 키는 기지국 또는 인증 서버에서 랜덤하게 생성한다. 그 기준은 이러한 서비스를 관리하는 범위에 따라 다른데, 그 범위가 단일 기지국일 경우에는 기지국이 GKEK와 트래픽 암호화 키를 생성하고 이와 반대로 망 전체적인 경우에는 인증 서버가 이 키들을 생성한다. 또한, GKEK의 일련번호와 유효 시간은 트래픽 암호화 키의 일련번호화 유효 시간과 동일하게 적용된다.

<55> 제 8도는 본 발명에서 제안하는 Key Update Command 메시지의 테이블이다.

<56> 이 Key Update Command 메시지는 Multicast 서비스와 Broadcast 서비스에 한해서 정의되는 메시지이고 다음과 같은 파라미터들이 포함된다.

<57> Key Update Command 메시지를 통해 새로이 분배할 트래픽 암호화 키와 관련된 인증키 일련 번호를 의미하는 Key-Sequence-Number와 해당 SA의 식별자인 SA ID가 존재한다.

<58> Key Update Command 메시지는 크게 두 가지의 역할을 하는데 이를 구별해주는 코드인 Key Push Modes가 있다.

<59> 또한, 도 7에서 정의하는 TEK-Parameters들이 포함되어 있고, 이 Key Update Command 메시지에 대한 인증 기능을 위한 HMAC-Digest가 포함된다.

<60> 특히, GKEK를 갱신하기 위해서 해당 서비스를 제공받고 있는 모든 단말 각각에게 전송하는 첫번째 Key Update Command 메시지와 트래픽 암호화 키를 갱신하기 위해서 해당 서비스를 제공받고 있는 모든 단말에게 동시에 전송하는 두번째 Key Update Command 메시지에 포함되는 파라미터들은 각각 다르다. 첫번째와 두번째 Key Update Command 메시지에는 TEK-Parameters를 제외한 인증키용 Key-Sequence-Number와 SA ID와 Key Push Modes 그리고 HMAC-Digest가 공히 포함되어 있다. 하지만, TEK-Parameters에 포함되어 있는 부파라미터들 중에서 GKEK와 트래픽 암호화 키용 Key-Sequence-Number는 첫번째 Key Update Command 메시지에 포함되고, 트래픽 암호화 키와 트래픽 암호화 키 유효 시간과 트래픽 암호화 키 일련 번호 그리고 CBC-IV는 두 번째 Key Update Command 메시지에 포함된다.

<61> 제 9도는 본 발명에서 제안하는 Key Update Command 메시지의 Key push modes 테이블이다.

<62> 이 Key push modes로써 Key Update Command 메시지의 용도를 구별해주는 코드이다. Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키를 갱신하는데 있어서 기지국은 두 번의 Key Update Command 메시지를 전송한다. 첫번째 Key Update Command메시지로는 GKEK를 갱신하기 위해 사용되고, 두번째 Key Update Command 메시지는 실질적인 트래픽 암호화 키를 갱신하기 위해 사용된다. 이 Key push modes에 따라 Key Update Command 메시지에는 8도와 같이 각각 다른 파라미터들을 포함한다.

<63> 제 10도는 본 발명에서 제안하는 Key Update Command 메시지의 파라미터인

HMAC-Digest 생성할 때 사용되는 입력키를 묘사하는 테이블이다.

<64> Key Update Command 메시지 자체를 인증하기 위해서 HMAC-Digest가 필요한데, 이 HMAC-Digest를 생성 시 사용되는 입력키는 Key Update Command 메시지에 따라 즉, Key push modes값에 따라 다르다.

<65> Multicast 서비스나 Broadcast 서비스를 제공 받는 모든 단말 각각에게 따로 전송하는 첫번째 Key Update Command 메시지, 즉 Key push modes값이 GKEK update mode일 때 HMAC-Digest를 만드는 입력 키는 해당 단말에게 미리 분배한 인증키이다. 이와는 달리, 위 서비스를 제공 받는 모든 단말에게 동시에 전송하는 두번째 Key Update Command 메시지, 즉 Key push modes값이 TEK update mode일 때 HMAC-Digest 입력 키는 GKEK update mode의 Key Update Command 메시지를 통해 분배한 GKEK이다. 이는 TEK update mode 의미의 Key Update Command 메시지는 방송적으로 전송하기 때문에, 서비스를 제공받고 있는 모든 단말이 이 메시지를 인증할 수 있어야 한다. 기지국뿐만 아니라 해당 서비스를 제공받고 있는 모든 단말이 안전하게 공유하고 있는 키는 GKEK이기 때문이다.

<66> 제 11도는 본 발명에서 제안하는 Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 갱신하는데 있어서 비정상적인 경우의 절차도이다.

<67> 단말이 최초로 임의의 Mutlicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키를 분배받는 절차 (S1111, S1112)는 도 4에서 단말의 최초 트래픽 암호화 키 분배 절차 (S411, S412)와 이 절차에 사용되는 메시지들의 내부 파라미터들도 동일하다.

<68> 이 후, 해당 서비스의 트래픽 데이터를 끊임없이 안전하게 기지국이 단말에게 제공하기 위해서 트래픽 암호화 키를 주기적으로 갱신해야 한다. 기지국은 M&B TEK Grace Time (ⓐ)을 기준으로 GKEK update mode의 Key Update Command 메시지와 TEK update mode의 Key Update Command 메시지를 해당 서비스를 제공받고 있는 모든 단말들에게 전송한다 (S1121, S1122, S1123). 단말들은 이 메시지들을 수신받음으로써 다음 주기의 트래픽 암호화 키를 분배받게 되는 것이다.

<69> 하지만, 단말들이 두 종류의 Key Update Command 메시지를 올바르게 수신하지 못 했을 경우, 즉 비정상적으로 트래픽 암호화 키를 분배받지 못한 단말들은 내부적으로 관리하고 있는 TEK Grace Time (ⓑ)이 동작하게 된다 (1122). 이 TEK Grace Time이 동작하는 단말들은 내부 트래픽 암호화 키 상태 머신에 TEK Refresh Timeout 이벤트가 발생한다 (S1131). 이 이벤트로 인해 비정상적으로 트래픽 암호화 키를 분배받지 못한 단말들은 다음 주기의 트래픽 암호화 키를 요구한다. 단말은 최초 트래픽 암호화 키 분배 절차와 동일하게 Key Request 메시지와 Key Reply 메시지를 교환함으로써 트래픽 암호화 키 갱신을 하게 된다 (S1132, S1133).

<70> 이 후, *x* 번째 트래픽 암호화 키의 유효 시간이 만료되면 해당 *x+1*번째의 트래픽 암호화 키 실제 유효 시간이 시작된다 (1112). 이 후부터 제공받은 해당 서비스 데이터는 *x+1*번째의 트래픽 암호화 키를 가지고 복호화하는 것이다.

<71> 본 특허에서 제안하는 Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키를 갱신하기 위해서 일반적으로 기지국이 Key Update Command 라는 메시지를 두 번 전송한다. 하지만, 이 메시지들을 제대로 수신받지 못해 비정상적인 경

우에 있는 단말들은 Key Request 메시지를 전송해서 트래픽 암호화 키를 요청하고 이에 대한 응답으로 기지국으로부터 Key Reply 메시지를 수신받음으로써 트래픽 암호화 키를 갱신하게 된다.

<72> 제 12도는 본 발명에서 제안하는 단말의 트래픽 암호화 키 요청 상황에 따른 Key Reply 메시지에 포함되어 전송되는 TEK-Parameters 정보를 나타내는 테이블이다.

<73> 도 11에서처럼 단말은 여러 시점에서 트래픽 암호화 키 요청 메시지인 Key Request 메시지를 전송할 수 있다.

<74> 단말이 임의의 Multicast 서비스나 Broadcast 서비스를 제공받기 위해서 트래픽 암호화 키를 어느 시점에서든지 Key Request 메시지를 통해 최초로 요구할 수 있다. 이 Key Request 메시지를 수신 받은 기지국은 내부적으로 관리하고 있는 M&B TEK Grace Time 시점을 기준으로 트래픽 암호화 키 응답 메시지인 Key Reply 메시지의 내부 파라미터들이 다르다. 도 6과 도 11에처럼 기지국은 M&B TEK Grace Time 시점 (ⓐ) 이전 에는 해당 서비스의 현재 주기 동안 유효한 TEK-Parameters가 포함된 Key Reply 메시지를 전송한다. 이와는 달리 M&B TEK Grace Time 시점 (ⓐ) 이후에는 해당 서비스의 현재 주기 동안 유효한 TEK-Parameters와 다음 주기 동안 유효한 TEK-Parameters가 포함된 Key Reply 메시지를 전송한다. 이는 모든 단말들에게 다음 주기 동안 유효한 트래픽 암호화 키를 공개하기 시점 (ⓐ) 이전에 기지국이 어떠한 단말들에게도 다음 주기 동안 유효한 트래픽 암호화 키 관련 파라미터인 TEK-Parameters 정보를 주지 않는다라는 장점뿐만 아니라 트래픽 암호화 키 응답

메시지인 Key Reply 메시지의 양도 줄일 수 있다라는 장점이 있다. 또한, 해당 서비스를 제공받고 있는 단말들에게 다음 주기 동안 유효한 트래픽 암호화 키를 공개한 시점 (ⓐ) 이후에 기지국은 트래픽 암호화 키를 요구한 단말들에게 현재뿐만 아니라 다음 주기 동안 유효한 TEK-Parameters를 전송함으로써 단말이 관리하고 있는 TEK Grace Time 시점 (ⓑ) 이후에 다음 주기 동안 유효한 트래픽 암호화 키 요청을 하지 않도록 하기 위함이다.

<75> 만약, TEK Grace Time 시점 (ⓑ) 이후에 단말이 트래픽 암호화 키를 요청하게 되면 기지국은 다음 주기 동안 유효한 TEK-Parameters만이 포함된 Key Reply 메시지를 전송한다. 이는 단말은 해당 서비스를 현재 받고 있기 때문에 현재 주기 동안 유효한 TEK-Parameters를 이미 가지고 있다라고 가정하는 것이다. 이로써, 트래픽 암호화 키 응답 메시지인 Key Reply 메시지에 불필요한 정보들을 줄일 수 있다라는 장점이 있다.

<76> 제 13도는 본 발명에서 제안하는 기지국이 트래픽 암호화 키 갱신을 시작하고 갱신된 트래픽 암호화 키를 분배하는 방식에서의 모든 서비스에 대한 트래픽 암호화 키 상태 머신 흐름에 대한 그림이다.

<77> 단말은 Unicast 서비스, Multicast 서비스 또는 Broadcast 서비스와 상관없이 모든서비스에 대하여 트래픽 암호화 키 상태 머신 흐름도의 흐름을 따르고 최대 두 개씩의 트래픽 암호화 키 상태 머신이 존재한다.

<78> 도 4와 같이 단말이 Multicast 서비스나 Broadcast 서비스를 제공받고자 할 때 해당 서비스에 대한 트래픽 암호화 키를 기지국으로 요청하고 기지국으로부터

이를 분배받는다 (S411, S412). 이와 같은 절차를 통해 단말은 해당 서비스용 트래픽 암호화 키를 기지국과 공유하게 되어 트래픽 암호화 키 상태 머신이 Operational 상태에 있게 된다.

<79> 기지국은 M&B TEK Grace Time 시점 이전에 해당 서비스를 이미 제공받고 있는 단말들에게 GKEK update mode의 Key Update Command 메시지를 전송한다 (S421). 이를 수신한 단말은 내부 트래픽 암호화 키 상태 머신에 GKEK Updated라는 이벤트를 발생시키고 이에 따라 M&B Rekey Interim Wait 상태에 머무르게 된다. 이 후, 기지국은 M&B TEK Grace Time 시점 이후에 TEK update mode의 Key Update Command 메시지를 방송으로 전송한다 (S423). 이를 수신한 단말은 내부 트래픽 암호화 키 상태 머신에 Key Updated라는 이벤트를 발생시키고 이에 따라 Operational 상태에 머무르게 된다. 하지만, TEK update mode의 Key Update Command 메시지를 제대로 수신받지 못한 단말은 내부적으로 관리하고 있는 TEK Grace Time 시점에 내부 트래픽 암호화 키 상태 머신에 TEK Refresh Timeout라는 이벤트를 발생시키고 Rekey Wait 상태에 머무르게 된다. 또한, 기지국으로 Key Request 메시지를 통해서 다음 주기 동안 유효한 트래픽 암호화 키를 요청한다.

<80> 이와는 달리, GKEK update mode의 Key Update Command 메시지와 TEK update mode의 Key Update Command 메시지를 제대로 수신하지 못한 단말은 TEK Grace Time 시점에 내부 트래픽 암호화 키 상태 머신에 TEK Refresh Timeout라는 이벤트를 발생시키고 Rekey Wait 상태에 머무르게 된다. 또한, 기지국으로 Key Request 메시지를 통해서 다음 주기 동안 유효한 트래픽 암호화 키를 요청한다.

<81> 제 14도는 본 발명에서 제안하는 기지국이 트래픽 암호화 키 갱신을 시작하고 갱신된 트래픽 암호화 키를 분배하는 방식에서의 모든 서비스에 대한 트래픽 암호화 키 상태 천이를 나타내는 테이블이다.

<82> 이는 도 13과 같이 서비스에 대한 트래픽 암호화 키 상태 흐름도를 테이블로 나타낸 것이다. 여기에서, 7-G 구간과 10-D 구간 그리고 11-G 구간은 오직 Multicast 서비스나 Broadcast 서비스에 한해서만 규정된다.

<83> 10-D 구간은 Multicast 서비스나 Broadcast 서비스를 제공받은 단말이 이미 해당 서비스용 트래픽 암호화 키를 분배받아서 내부적으로 관리하고 있는 트래픽 암호화 키 상태 머신이 Operational 상태일 때, 기지국으로부터 해당 서비스에 대한 GKEK update mode의 TEK Update Command 메시지를 수신함으로써 M&B Rekey Interim Wait 상태에 머물게 된다.

<84> 11-G 구간은 단말의 트래픽 암호화 키 상태 머신이 M&B Rekey Interim Wait 상태일 때, 기지국으로부터 해당 서비스에 대한 TEK update mode의 TEK Update Command 메시지를 수신함으로써 Rekey Wait 상태에 머물게 된다.

<85> 또한, 7-G 구간은 단말의 트래픽 암호화 키 상태 머신이 M&B Rekey Interim Wait 상태일 때, 기지국으로부터 해당 서비스에 대한 TEK update mode의 TEK Update Command 메시지를 수신하지 못함으로써 Operational 상태에 머물게 된다.

【발명의 효과】

<86> 본 발명은 IEEE 802.16 WirelessMAN 시스템에서 Multicast 서비스나

Broadcast 서비스용 트래픽 암호화 키를 관리하는 메커니즘을 정의하는 것으로, 다음과 같은 효과가 있다.

<87> 첫째, Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키 갱신을 기지국이시작하여 갱신된 키를 해당 서비스를 제공받는 단말들에게 Broadcast Connection을 통해 전달함으로써, 적은 신호 자원을 가지고도 트래픽 암호화 키를 갱신 및 분배가 가능하다.

<88> 둘째, 기지국이 상기 서비스들의 트래픽 암호화 키를 갱신하고 단말에게 일률적으로 분배하는 방식을 사용함으로써, 단말로부터 일시적인 트래픽 암호화 키 요청 메시지를 사용하지 않고 두 번의 Key Update Command 메시지로 모든 단말에게 트래픽 암호화 키를 분배하게 되어 기지국 입장에서 이러한 트래픽 암호화 키와 관련된 처리량이 감소된다는 장점이 있다.

<89> 셋째, 기지국이 트래픽 암호화 키를 갱신하는데 있어서, 트래픽 암호화 키 자체를 암호하기 위해 필요한 GKEK를 단말의 인증키로 암호화해서 모든 단말 각각에게 전송하기 때문에 GKEK를 안전하게 분배할 수 있다.

<90> 넷째, 트래픽 암호화 키를 모든 단말에게 Broadcast하게 전송할지라도 트래픽 암호화 키 자체도 GKEK로 암호화했기 때문에, 오직 GKEK를 분배받은 단말들만 트래픽 암호화 키를 복호할 수 있어서 안전하다라는 장점이 있다.

<91> 다섯째, Multicast 서비스와 Broadcast 서비스용 트래픽 암호화 키를 기지국에서 주기적으로 갱신함으로써 상기 서비스에 대한 강력한 보안을 유지하면서 단말에게 서비스를 제공할 수 있다.

<92> 여섯째, Multicast 서비스의 경우 Multicast 서비스마다 관련된 SA 특히 트래픽 암호화 키가 다르므로 Multicast 서비스마다 보안 유지가 가능하다.

【특허청구범위】

【청구항 1】

IEEE 802.16 WirelessMAN 기반의 무선 인터넷 시스템에서 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키를 관리하는 방법.

【청구항 2】

제 1항에 있어서, Multicast 서비스나 Broadcast 서비스는 각각 하나의 독립적이고 고유한 SA에 매핑하는 방법.

【청구항 3】

제 1항에 있어서, 기지국이 Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키 갱신을 시작하는 방법.

【청구항 4】

제 3항에 있어서, Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키가 만료되기 전 기지국이 트래픽 암호화 키 갱신을 시작하는 시간인 M&B TEK Grace Time을 사용하는 방법.

【청구항 5】

제 4항에 있어서, 기지국의 M&B TEK Grace Time 값이 단말의 TEK Grace Time 값보다 큰 값으로 설정함으로써, 단말이 Multicast 서비스나 Broadcast 서비스용 트래픽 암호화 키에 대하 갱신을 시작하기 전에 기지국이 먼저 시작하는 방법.

【청구항 6】

제 5 항에 있어서, 기지국이 Multicast 서비스나 Broadcast 서비스에 대한 트래픽암호화 키를 갱신 및 분배하기 위해서 두 번의 Key Update Command 메시지를 사용하는 방법.

【청구항 7】

제 3항과 제 4항에 있어서, 기지국이 M&B TEK Grace Time 시점 이전에 해당 Multicast 서비스나 Broadcast 서비스에 대한 GKEK를 해당 서비스를 제공받고 있는 단말 각각에게 전송하는 방법.

【청구항 8】

제 7항에 있어서, GKEK는 트래픽 암호화 키를 암호하는데 있어서 필요한 입력키로 사용하는 방법.

【청구항 9】

제 7항에 있어서, GKEK는 기지국이 이미 각각의 단말에게 분배한 인증키를 가지고 암호화되어 전송되는 방법.

【청구항 10】

제 7항에 있어서, GKEK는 기지국 또는 인증 서버가 랜덤하게 생성하는 방법.

【청구항 11】

제 10항에 있어서, 임의의 Multicast 서비스나 Broadcast 서비스의 범위가 하나의 기지국에 국한될 때에는 GKEK를 기지국이 랜덤하게 생성하는 방법.

【청구항 12】

제 10항에 있어서, 임의의 Multicast 서비스나 Broadcast 서비스의 범위가 네트웍 전체일때에는 GKEK를 인증 서버가 랜덤하게 생성하는 방법.

【청구항 13】

제 7항에 있어서, 기지국이 해당 서비스를 제공받고 있는 단말 각각에게 전송할 때 Key Update Command 메시지를 Primary Management Connection을 통해 전송하는 방법.

【청구항 14】

제 3항과 제 4항에 있어서, 기지국이 내부적으로 관리하고 있는 M&B TEK Grace Time 시점에 내부 트래픽 암호화 키 상태 머신에 M&B TEK Refresh Timeout 이벤트를 발생시키는 방법.

【청구항 15】

제 3항과 제 4항 그리고 제 14항에 있어서, 기지국은 내부 트래픽 암호화 키 상태 머신에 M&B TEK Refresh Timeout 이벤트로 인해 모든 단말들에게 트래픽 암호화 키를 전송하는 방법.

【청구항 16】

제 15항에 있어서, 기지국은 트래픽 암호화 키를 GKEK를 가지고 암호화하여 전송하는 방법.

【청구항 17】

제 15항에 있어서, 기지국은 Key Update Command 메시지를 통해 모든 단말에게 방송적으로 트래픽 암호화 키를 전송하는 방법.

【청구항 18】

제 13항과 제 17항에 있어서, 두 개의 Key Update Command 메시지를 통해 GKEK와 트래픽 암호화 키를 수신한 단말들은 내부적으로 관리하고 있는 TEK Grace Time 타이머를 동작시키지 않는 방법.

【청구항 19】

제 3항에 있어서, 기지국과 단말이 새로운 트래픽 암호화 키를 올바르게 갱신하고 난 이후 현재 사용중인 트래픽 암호화 키에 대한 유효 시간 종료 후 새로운 트래픽 암호화 키에 대한 유효 시간을 설정하는 방법.

【청구항 20】

제 3항에 있어서, 기지국과 단말이 새로운 트래픽 암호화 키를 올바르게 갱신하고 난 이후 현재 사용중인 트래픽 암호화 키에 대한 유효 시간 종료 후 새로운 트래픽 암호화 키에 대한 유효 시간을 설정하는 방법.

【청구항 21】

제 1항에 있어서, 단말이 트래픽 암호화 키를 요청하기 위해 Key Request 메시지를 사용하고 이에 대한 응답으로 기지국이 트래픽 암호화 키를 분배하기 위해 Key Reply 메시지를 사용하는 방법.

【청구항 22】

제 21항에 있어서, 트래픽 암호화 키 응답 메시지인 Key Reply 메시지의 파라미터인 TEK-Parameters 파라미터에 내부 필드인 GKEK를 추가하는 방법.

【청구항 23】

제 22항에 있어서, 트래픽 암호화 키 응답 메시지인 Key Reply 메시지의 파라미터인 TEK-Parameters 파라미터에 내부 필드인 트래픽 암호화 키를 암호화하는 방법.

【청구항 24】

제 23항에 있어서, 트래픽 암호화 키를 암호화하는데 있어서 입력키로써 Unicast 서비스는 단말에 분배한 인증키로부터 만들어진 KEK를 사용하는 반면, Multicast 서비스난 Broadcast 서비스는 단말에 분배한 GKEK를 사용하는 방법.

【청구항 25】

제 3항에 있어서, Multicast 서비스나 Broadcast 서비스에 있어서 트래픽 암호화 키를 기지국이 갱신하여 분배하기 위해서 Key Update Command 메시지를 사용하는 방법.

【청구항 26】

제 25항에 있어서, Key Update Command 메시지에 있어서 단말 인증키 일련번호, SA의 식별자인 SAID, Key Update Command 메시지의 사용 코드를 구별시켜주는 Key push modes, 트래픽 암호화 키와 관련된 정보인 TEK-Parameters 그리고 Key

Update Command 메시지 자체를 인증하기 위한 HMAC-Digest를 포함시키는 방법.

【청구항 27】

제 26항에 있어서, Key Update Command 메시지의 사용 코드를 구별시켜주는 Key push modes 파라미터에는 GKEK를 분배하는 의미를 포함하는 GKEK update mode와 트래픽 암호화 키를 분배하는 의미를 포함하는 TEK update mode를 사용하는 방법.

【청구항 28】

제 6항과 13항과 제 17항 그리고 제 27항에 있어서, GKEK를 분배하는 첫 번째의 Key Update Command 메시지의 Key push modes는 GKEK update mode를 사용하고 트래픽 암호화 키를 분배하는 두번째의 Key Update Command 메시지의 Key push modes는 TEK update mode를 사용하는 방법.

【청구항 29】

제 6항과 제 26항에 있어서, 두 번의 모든 Key Update Command 메시지에 인증 키 일련 번호, SAID, Key Push Modes, HMAC-Digest는 포함하는 방법.

【청구항 30】

제 6항과 제 26항에 있어서, 첫번째 Key Update Command 메시지에는 내부 파라미터인 TEK-Parameters에서 GKEK와 트래픽 암호화 키 일련 번호를 포함시키는 방법.

【청구항 31】

제 6항과 제 26항에 있어서, 두번째 Key Update Command 메시지에는 내부 파라미터인 TEK-Parameters에서 트래픽 암호화 키, 트래픽 암호화 키 유효 시간, 트래픽 암호화 키 일련 번호와 CBC-IV를 포함시키는 방법.

【청구항 32】

제 31항에 있어서, GKEK는 각 단말마다 가지고 있는 인증키로 암호화하고 트래픽 암호화 키는 GKEK로 암호화하는 방법.

【청구항 33】

제 3항과 제 6항에 있어서, 서비스를 제공받고 있는 단말이 두 번의 Key Update Command 메시지 중 최소한 하나라도 제대로 수신 받지 못한 경우 트래픽 암호화 키를 갱신하는 방법.

【청구항 34】

제 33항에 있어서, 서비스를 제공받고 있는 단말이 두 번의 Key Update Command 메시지 중 최소한 하나라도 제대로 수신 받지 못한 경우 단말 내부적으로 관리하고 있는 TEK Grace Time을 동작시키는 방법.

【청구항 35】

제 34항에 있어서, TEK Grace Time의 동작으로 인해 단말의 내부 트래픽 암호화 키 상태 머신에 TEK Refresh Timeout 이벤트를 발생시키는 방법.

【청구항 36】

제 35항에 있어서, TEK Refresh Timeout 이번트로 인해 단말이 트래픽 암호화 키 갱신을 시작하는 방법.

【청구항 37】

제 33항과 제 36항에 있어서, 단말이 트래픽 암호화 키 갱신을 시작하는 경우 Key Request 메시지를 이용하고 이에 대한 응답으로 기지국은 Key Reply 메시지를 이요하는 방법.

【청구항 38】

제 3항, 제 4항, 제 21항, 제 33항과 제 34항에 있어서, 단말이 임의의 Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키를 최초로 요구하는 경우에 기지국은 M&B TEK Grace Time 시점 이전에는 현재 기간 동안 유효한 트래픽 암호화 키를 분배하고 M&B TEK Grace Time 시점 이후에는 현재 기간 동안뿐만 아니라 다음 기간 동안 유효한 트래픽 암호화 키를 분배하는 방법.

【청구항 39】

제 3항, 제 4항, 제 21항, 제 33항과 제 34항에 있어서, 단말이 임의의 Multicast 서비스나 Broadcast 서비스에 대한 트래픽 암호화 키를 제대로 수신받지 못해서 트래픽 암호화 키 갱신을 요구하는 경우에 기지국은 다음 기간 동안 유효한 트래픽 암호화 키를 분배하는 방법.

【청구항 40】

제 3항, 제 4항, 제 21항, 제 33항과 제 34항에 있어서, 단말이 내부 트래픽 암호화 키 상태 머신을 관리하는 방법.

【청구항 41】

제 40항에 있어서, 단말이 기지국으로부터 갱신된 GKEK를 제대로 수신한 경우내부 트래픽 암호화 키 상태 머신에 GKEK Updated 이벤트를 발생시키고 트래픽 암호화 키를 제대로 수신한 경우 내부 트래픽 암호화 키 상태 머신에 TEK Updated 이벤트를 발생시키는 방법.

【청구항 42】

제 41항에 있어서, 트래픽 암호화 키 상태 머신이 Operational 상태에 있는 단말이 기지국으로부터 갱신된 GKEK를 제대로 수신한 경우 M&B Rekey Interim Wait 상태에 머무르는 방법.

【청구항 43】

제 41항에 있어서, 트래픽 암호화 키 상태 머신이 M&B Rekey Interim Wait 상태에 있는 단말이 기지국으로부터 갱신된 트래픽 암호화 키를 제대로 수신한 경우 Operational 상태에 머무르는 방법.

【청구항 44】

제 41항과 제 43항에 있어서, 트래픽 암호화 키 상태 머신이 M&B Rekey Interim Wait 상태에 있는 단말이 기지국으로부터 갱신된 트래픽 암호화 키를 제대

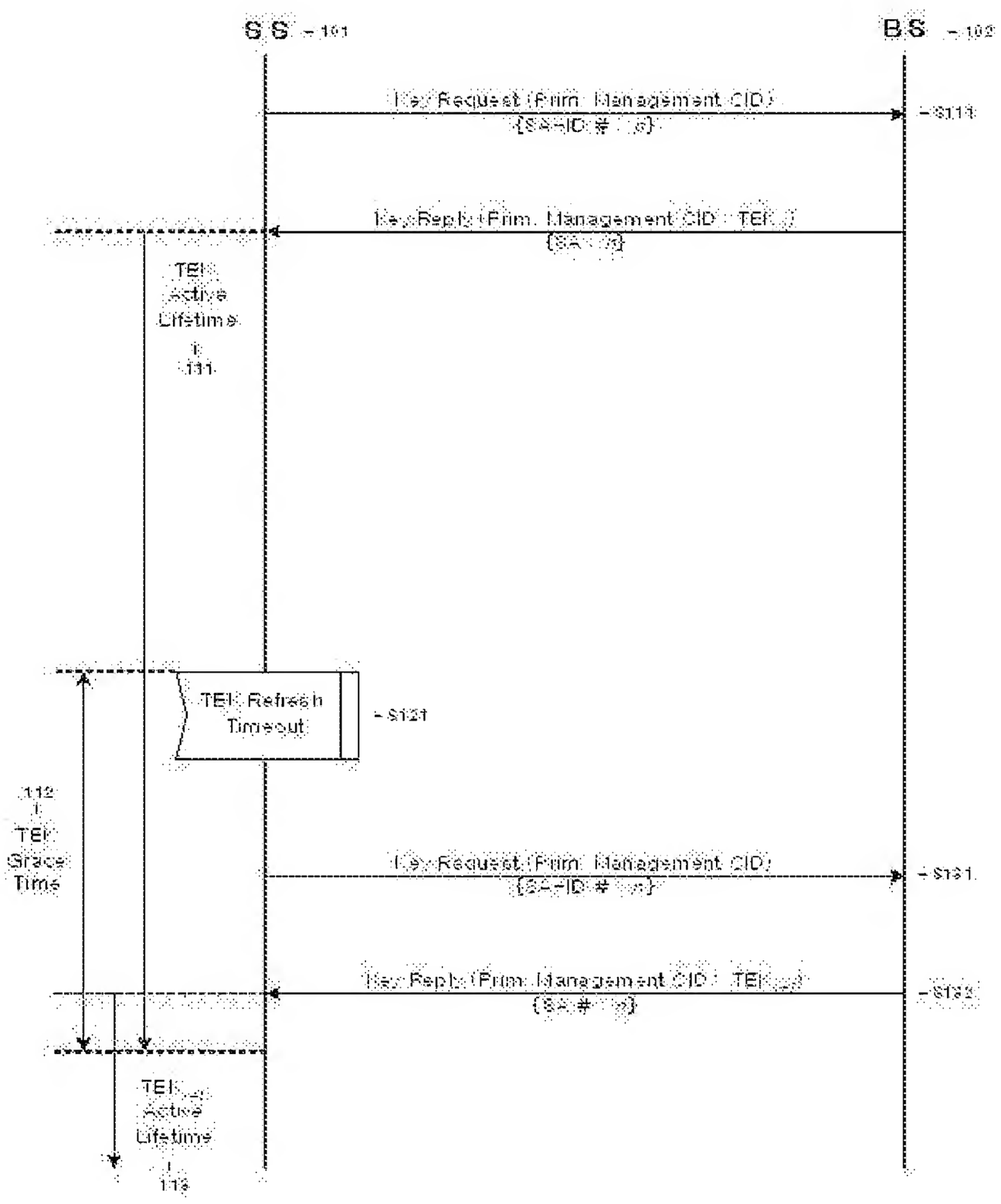
로 수신하지 못한 경우 TEK Refresh Timeout 이벤트를 발생시키고 Rekey Wait 상태로 옮기고 단말은 기지국에게 Key Request 메시지를 통해 트래픽 암호화 키를 요청하는 방법.

【청구항 45】

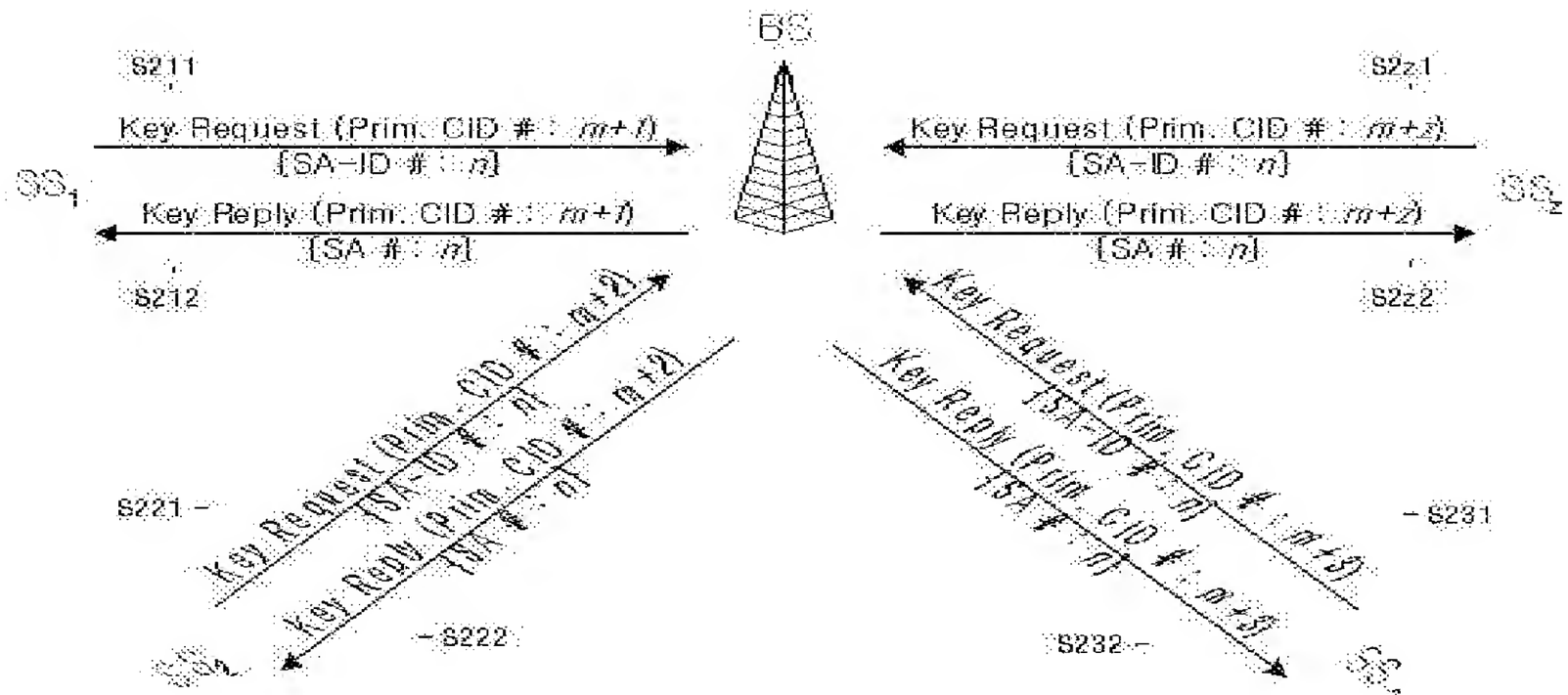
제 40항에 있어서, 트래픽 암호화 키 상태 머신이 Operational 상태에 있는 단말이 기지국으로부터 GKEK 또는 트래픽 암호화 키를 제대로 수신하지 못한 경우 TEK Refresh Timeout 이벤트를 발생시키고 Rekey Wait 상태로 옮기고 단말은 기지국에게 Key Request 메시지를 통해 트래픽 암호화 키를 요청하는 방법.

【도면】

【도 1】


SS
101
BS
102
Key Request (Prim: Management CID)
{SA-ID # : n}
S111
Key Reply (Prim: Management CID : TEK)
{SA : n}
TEK
Active
Lifetime
111
TEK Refresh
Timeout
S121
112
TEK
Grace
Time
Key Request (Prim: Management CID)
{SA-ID # : n}
S131
Key Reply (Prim: Management CID : TEK)
{SA # : n}
S132
TEK
Active
Lifetime
113

【도 2】

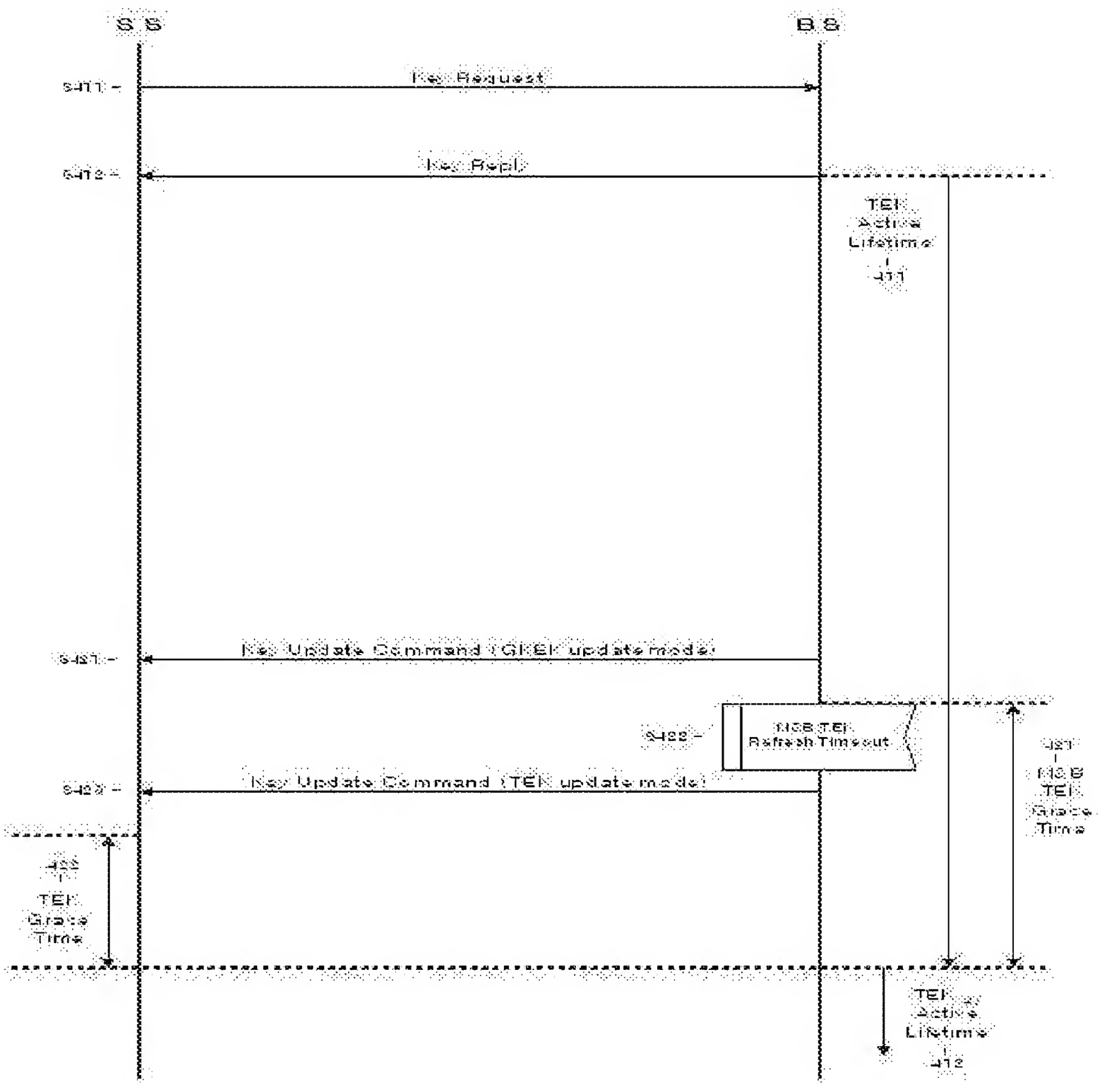


【도 3】

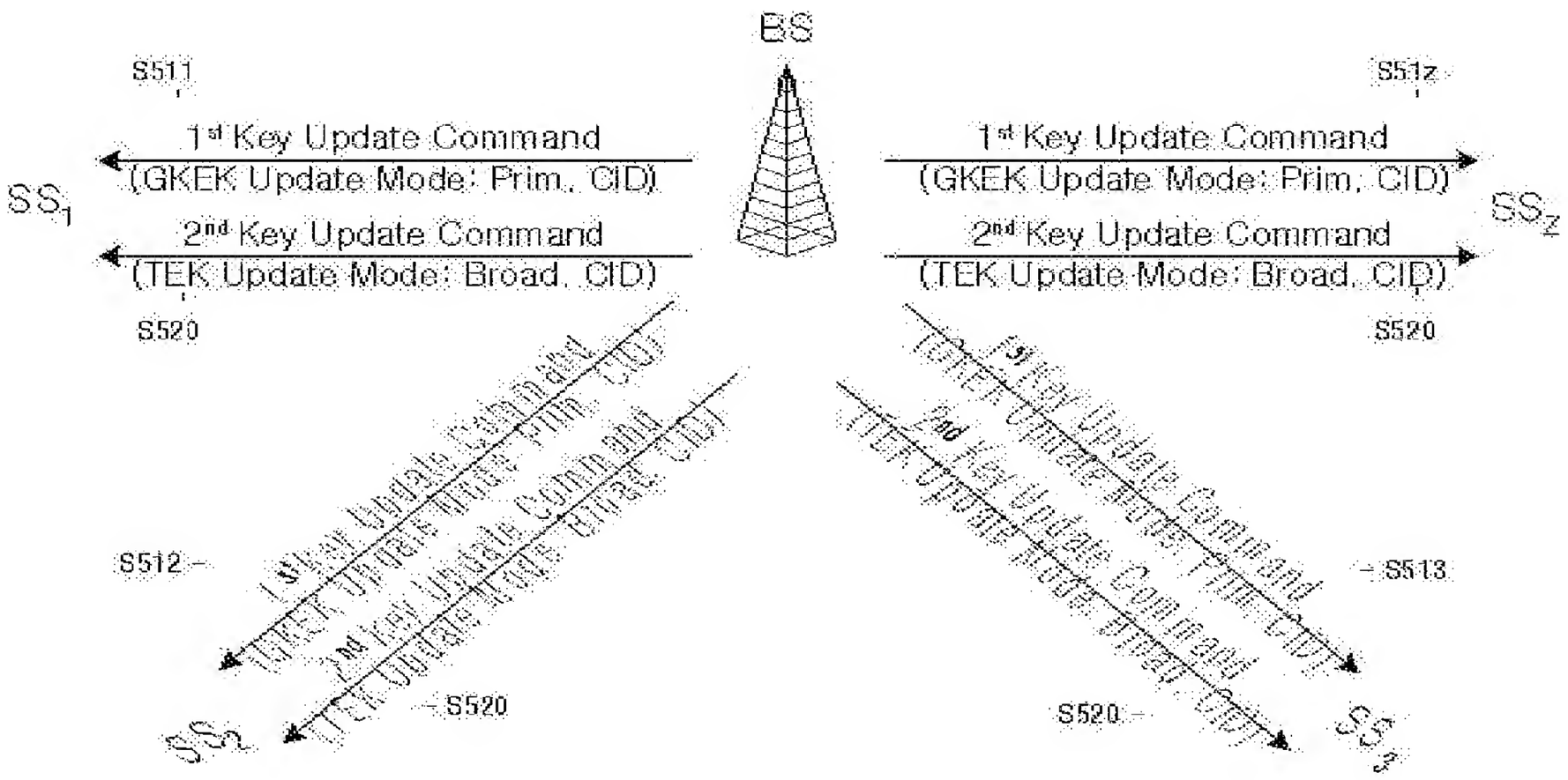
Operational ranges for privacy configuration setting - 300

System	Name	Description	Minimum value	Default value	Maximum value
BS	M&B TEK Grace Time	Time prior to TEK (for the multicast and broadcast traffic service) expiration BS begins rekeying. This time is longer than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value

【도 4】


SS
BS
S411
Key Request
S412
Key Reply
TEK Active Lifetime 411
S421
Key Update Command (GKEK update mode)
S422
RGB TEI Refresh Timeout
S423
Key Update Command (TEK update mode)
421 RGB TEI Grace Time
422 TEK Grace Time
TEK Active Lifetime 412

【도 5】



【도 6】

Key Reply Attributes – 600

Attribute	Contents
Key-Sequece-Number	Authorization key sequence number
SAID	Security Association ID
TEK-Paramters	“Older” generation of key parameters relevant to SAID
TEK-Parameters	“Newer” generation of key parameters relevant to SAID
HMAC-Digest	Keyed SHA messge digest

【도 7】

TEK-parameters subattributes – 700

Attribute	Contents
GKEK	GKEK, encrypted with the AK
TEK	TEK, encrypted with the GKEK (Multicast or Broadcast Service) or encrypted with the KEK (Unicast Service)
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequnce Number
CBC-IV	Cipher Block Chaining (CBC) Initialization Vector

【도 8】

Key Update Command Attributes – 800

Attribute	Contents	1st Message (Primary)	2nd Message (Broadcast)
Key-Sequece-Number	Authorization key sequence number	○	○
SAID	Security Association ID	○	○
Key Push Modes	Usage code of Key Update Command message	○	○
TEK-Parameters	"Newer" generation of key parameters relevant to SAID		
> GKEK	GKEK, encrypted with the AK	○	x
> TEK	TEK, encrypted with the GKEK (Multicast or Broadcast Service)	x	○
> Key-Lifetime	TEK Remaining Lifetime	x	○
> Key-Sequence-Number	TEK Sequnce Number	○	○
> CBC-IV	Cipher Block Chaining (CBC) Initialization Vector	x	○
HMAC-Digest	Keyed SHA messge digest	○	○

【도 9】

Key push modes – 900

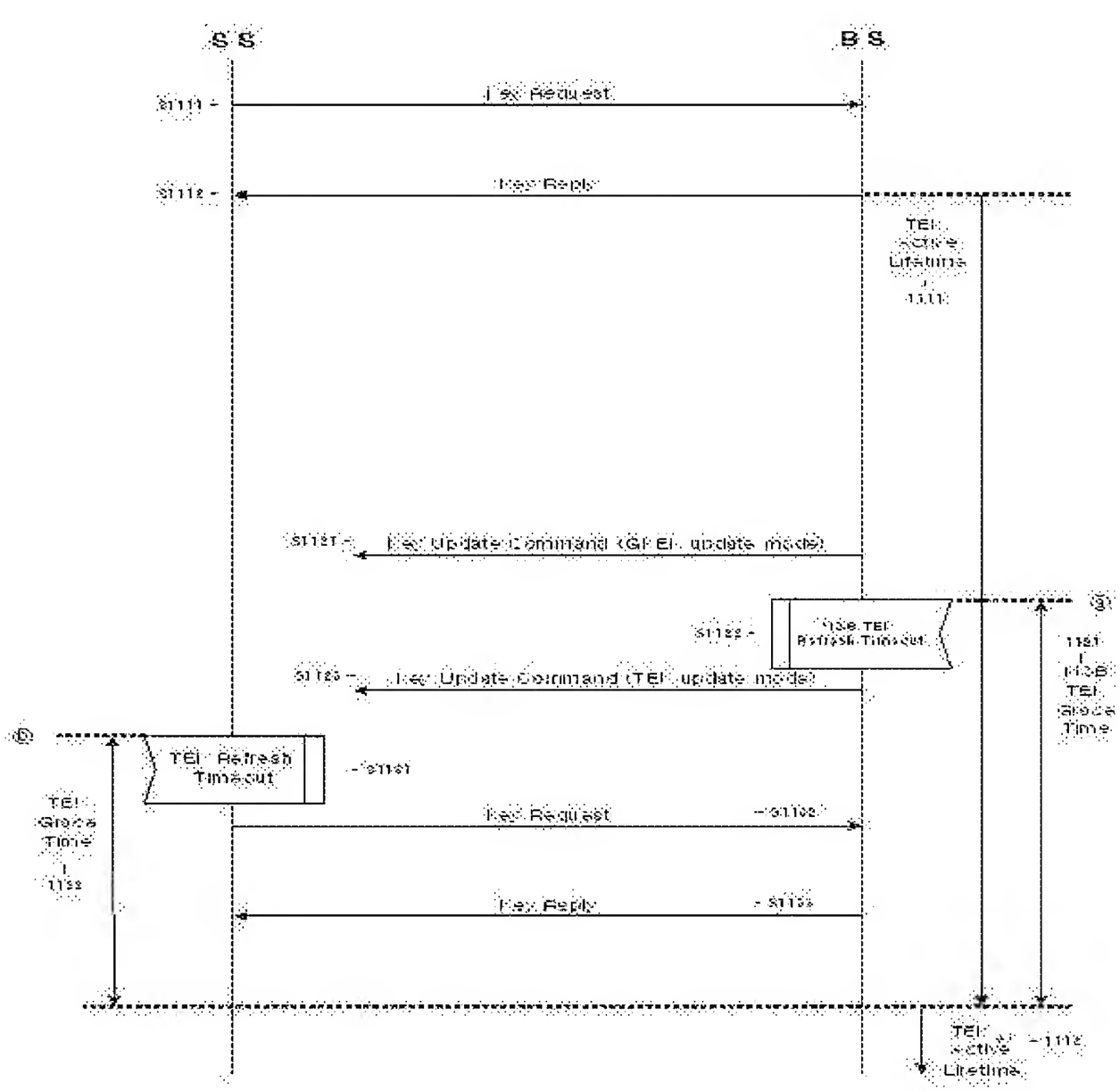
Type	Length	Value
30	1	0, GKEK update mode (1st message) 1, TEK update mode (2nd message) 2-255, reserved

【도 10】

Input Key of HMAC-Digest – 900

Key push modes	Input Key
GKEK update mode	AK
TEK update mode	GKEK

【도 11】



【도 12】

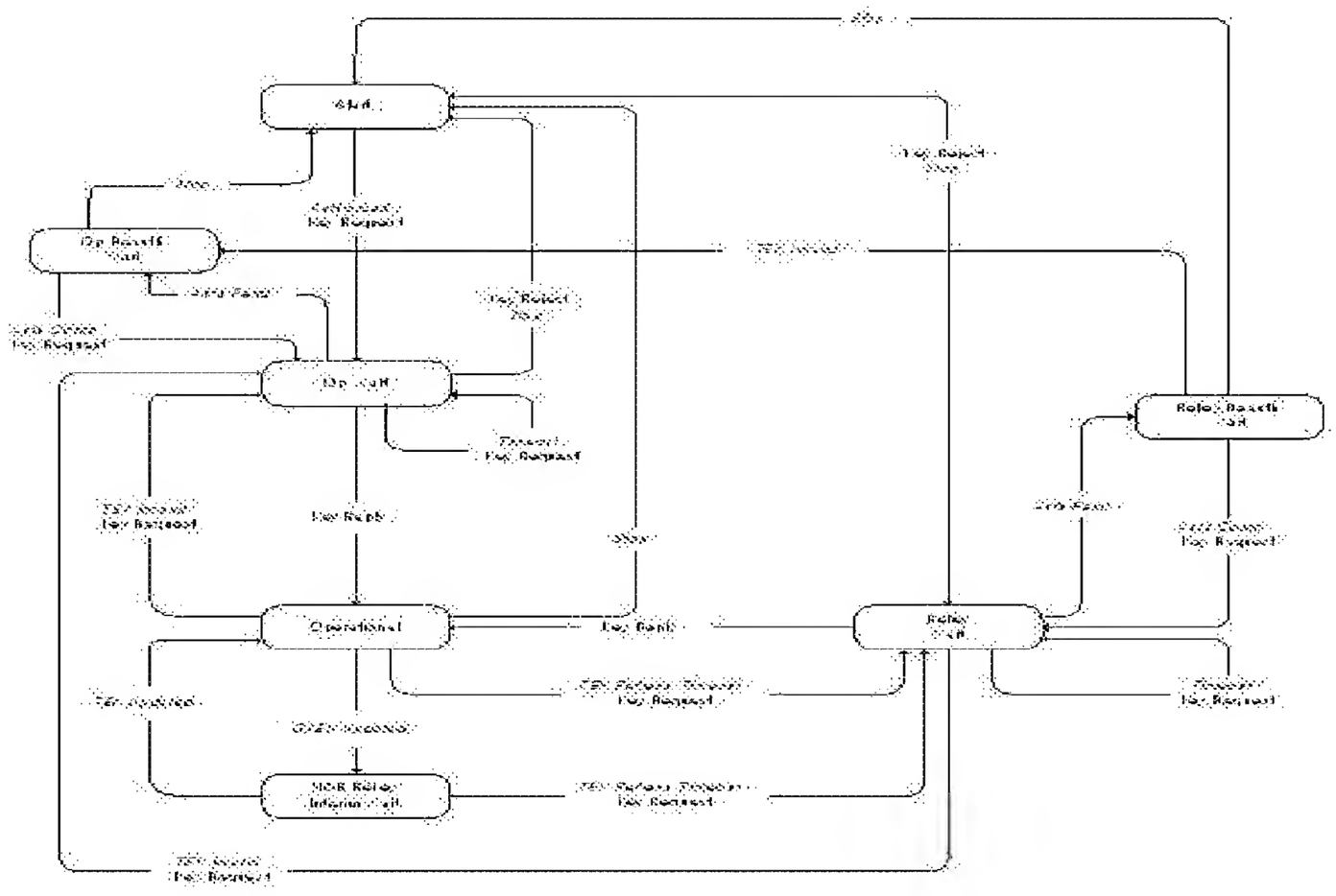
Transferred TEK-parameters generation information – 1200

Situation	Transferred TEK-parameter information
Initial TEK response (before ⓐ)	$TEK\text{-}Parameters_C$
Initial TEK response (after ⓐ)	$TEK\text{-}Parameters_C$ & $TEK\text{-}Parameters_N$
TEK update response (after ⓑ)	$TEK\text{-}Parameters_N$

C: Current generation of key parameters relevant to SAID

N: Next generation of key parameters relevant to SAID

【도 13】



【도 14】

TEK FSM state transition matrix

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait	(G) M&B Rekey Interim Wait
(1) Stop		Start	Start	Start	Start	Start	
(2) Authorized	Op Wait						
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait		
(4) Auth Comp			Op Wait			Rekey Wait	
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait	
(6) Timeout		Op Wait			Rekey Wait		
(7) TEK Refresh Timeout				Rekey Wait			Rekey wait
(8) Key Reply		Operational			Operational		
(9) Key Reject		Start			Start		
(10) GKEK Updated				M&B Rekey Interim Wait			
(11) TEK Updated							Operational